

9 - isolation means (4) between the input/output module (2) and the encryption  
10 module (3), for making the sensitive information stored in the encryption module (3)  
11 inaccessible to the host system (HS) and for ensuring the parallelism of the operations  
12 performed by the input/output module (2) and the encryption module (3).

1 16. An encryption circuit according to claim 15, characterized in that the  
2 isolation means (4) of the circuit (1) comprises a double-port memory (4).

1 17. An encryption circuit according to claim 15 wherein this isolation means  
2 (4) comprises a double port memory coupled between the input/output module (2) and  
3 the encryption module (3), the dual-port memory (4) being coupled to a first bus and  
4 adapted to simultaneously handle the exchange of data, commands and statuses'  
5 between the input/output and encryption modules (2 and 3), and isolation between the  
6 two modules (2 and 3).

1 18. An encryption circuit is set forth in claim 15, characterized in that the  
2 encryption module (3) comprises:

3 - a first encryption sub-module (3<sub>1</sub>), dedicated to the processing of symmetric  
4 encryption algorithms, and being coupled with the first bus of the dual port memory  
5 (4);

6 - a second encryption sub-module (3<sub>2</sub>), dedicated to the processing of  
7 asymmetric encryption algorithms (40) and being coupled with the first bus of the  
8 dual-port memory (4) and including a separate internal second bus isolated from the  
9 first bus of the dual-port memory (4); and

10 - a CMOS memory (11) coupled with the dual-port memory (4) via the first  
11 bus of the dual-port memory containing the encryption keys.

1 19. An encryption circuit as set forth in claim 16, characterized in that the  
2 encryption modules (3) comprises:

3 - a first encryption sub-module (3<sub>1</sub>), dedicated to the processing of symmetric  
4 encryption algorithms, and being coupled with the first bus of the dual port memory  
5 (4);

6 - a second encryption sub-module (3<sub>2</sub>), dedicated to the processing of  
7 asymmetric encryption algorithms (40) and being coupled with the first bus of the  
8 dual-port memory (4) and including a separate internal second bus isolated from the  
9 first bus of the dual-port memory (4); and

10 - a CMOS memory (11) coupled with the dual-port memory (4) via the first  
11 bus of the dual-port memory containing the encryption keys.

1 20. An encryption circuit as set forth in claim 17, characterized in that the  
2 encryption module (3) comprises:

3 - a first encryption sub-module (3<sub>1</sub>), dedicated to the processing of symmetric  
4 encryption algorithms, and being coupled with the first bus of the dual port memory  
5 (4);

6 - a second encryption sub-module (3<sub>2</sub>), dedicated to the processing of  
7 asymmetric encryption algorithms (40) and being coupled with the first bus of the  
8 dual-port memory (4) and including a separate internal second bus isolated from the  
9 first bus of the dual-port memory (4); and

10 - a CMOS memory (11) coupled with the dual-port memory (4) via the first  
11 bus of the dual-port memory containing the encryption keys.



1 26. An encryption circuit according to claim 25, characterized in that the  
2 encryption component (9) comprises a field programmable array (FPGA).

1 27. An encryption circuit according to claim 26, characterized in that the  
2 second encryption sub-module (3<sub>2</sub>) comprises a flash memory PROM (12) and an  
3 SRAM memory (13) coupled with the second internal bus of the sub-module (3<sub>2</sub>).

1 28. An encryption circuit according to claim 21, further comprising a CMOS  
2 memory (11) containing security keys and security mechanisms (15) adapted to  
3 trigger a reset mechanism of the CMOS memory (11) in case of an alarm.

1 29. an encryption circuit according to claim 15 characterized in that the  
2 input/output module (2) comprises:

3 - a microcontroller (6) having an input/output processor (6<sub>1</sub>) and a PCI  
4 interface (6<sub>2</sub>) integrating DMA channels responsible for executing the data transfers  
5 between the host system (HS) and the circuit (1);

6 - a flash memory (7) containing the code of the input/output processor (6<sub>1</sub>) and  
7 a PCI interface (6<sub>2</sub>) integrating DMA channels responsible for executing the data  
8 transfers between the host system (HS) and the circuit (1);

9 - a flash memory (7) containing the code of the input/output processor (6<sub>1</sub>);  
10 and

11 - an SRAM memory (8) that receives a copy of the contents of the flash  
12 memory (7) upon startup of the input/output processor (6<sub>1</sub>).